Triakis Corporation

Project Technical Documentation
Description Document

For the Project Entitled:

The use of a Virtual System Simulator and Executable Specifications to Enhance Software Validation, Verification, and Safety Assurance

A NASA CI03
SARP Initiative 583
IVV-70 Project

Table of Contents

Table of Figures

1. Introduction

This document has been developed in support of a research project funded by the NASA Software Assurance Research Program (SARP) during the fiscal year 2003 Center Initiatives (CI03) effort. Triakis will create a simulation of the Shuttle Remote Manipulator System (SRMS) to be used as a vehicle for exploring the concepts described in section 2 of Triakis proposal number TC_G020614.

Project Abstract

Triakis' has created a simulation tool called IcoSim© that has proven to be extremely thorough at facilitating avionics systems and software design, validation, verification and certification. Through repeated application of IcoSim© on avionics development projects, Triakis has conceived a new approach to the avionics development process based on the creation, simulation and V&V of executable specifications (ES').

ES' are currently being studied as a means of reducing errors in defining requirements and communicating them to the team responsible for implementing designs. An IcoSim© ES unambiguously describes the functional performance of the system element that it simulates, and forms the functional requirements specification for detailed design. A HW design is simulated for each ES with sufficient fidelity to execute the SW object code developed to implement the specified requirements. The simulated HW running the SW object code, referred to as a detailed executable (DE), is plug-in compatible with the ES allowing the SW to be developed and tested in the same system environment in which the ES was developed, using the same system-level test scripts. Triakis' ES concept is described in greater detail in a white paper entitled *Verification & Validation of Embedded Systems & Software Using Executable Specifications & Detailed Executables in a Virtual System Integration Laboratory Environment*.

To date Triakis has developed its concept of the ES and tested elements of it on various avionics development projects but has yet to validate these ideas in a complete and comprehensive manner. The objective of our research is to test the validity of our ideas described in attachment II, on a small but non-trivial system and SW project from start to finish. We will explore the viability and benefits of using this development approach as it relates to systems and SW IV&V, quality, testability and reliability. We will also explore how the V&V process in the ES simulation environment uncovers functional deficiencies in both the SW and the system implementation, directing the creation of additional tests and/or design changes.

1.1 Purpose

This document has been created to provide a description of, and index into the technical documentation that Triakis intends to produce in support of the SARP initiative 583 project. Triakis is creating a simulation of a non-trivial system for use in its research. The information provided herein will help avoid confusion when trying to understand the relationship between technical documents, and their context within the project framework.

1.2 Scope

The documents described herein are limited to those technical documents that will be produced for the SARP initiative 583 research project. Administrative and other non-technical documents associated with the project are not included in the scope of in this document.

1.3 Definitions, Acronyms, And Abbreviations

CI03	Center Initiative for fiscal year 2003
DE	Detailed Executable
ES	Executable Specification
IV&V	Independent Verification and Validation

NASA	National Aeronautics & Space Administration
OSMA	Office of Safety and Mission Assurance
SARP	Software Assurance Research Program
SRMS	Shuttle Remote Manipulator System
SW	Software
SyDD	System Design Document
SyRS	System Requirements Specification
VSIL	Virtual System Integration Laboratory

1.4 References

TC_G020614 Triakis proposal to NASA for the SARP (Solicitation No: NRA SARP 0201) 14 June 2002

WP_020610d Verification & Validation of Embedded Systems & Software Using Executable Specifications & Detailed Executables in a Virtual System Integration Laboratory Environment

2. Project Technical Document Organization

The relational structure of the technical documents created for this project is shown in figure 1. The first eight characters in the document nomenclature identify the initiative number given to this project (SARP initiative 583). The first digit of the last three identifies the hierarchical level of the document while the last two identify each document within the level. The interconnecting lines and arrows indicate the requirements and information flow between the documents.

3. Document Descriptions

The following document descriptions are grouped according to document hierarchy as indicated in figure 1.

3.1 High-level Requirements Documents

3.1.1 SARP-I583-001 System Requirements Specification

The SyRS identifies the functional requirements for the system that will be developed. These requirements have been developed from the project description outlined in project proposal TC_G020614. Since this system is intended to be implemented in a virtual environment only, many requirements necessary for creating a real-world system have been omitted.

3.1.2 SARP-I583-002 Simulator Requirements Specification

The SiRS identifies the requirements necessary for developing a simulator that will create the virtual environment in which the target system will operate. This specification is created from information found in the SyRS and the project proposal.

3.2 High-level Design Documents

3.2.1 SARP-I583-101 System Design Document

The SyDD is used to document the system design developed to implement the requirements identified in the SyRS.

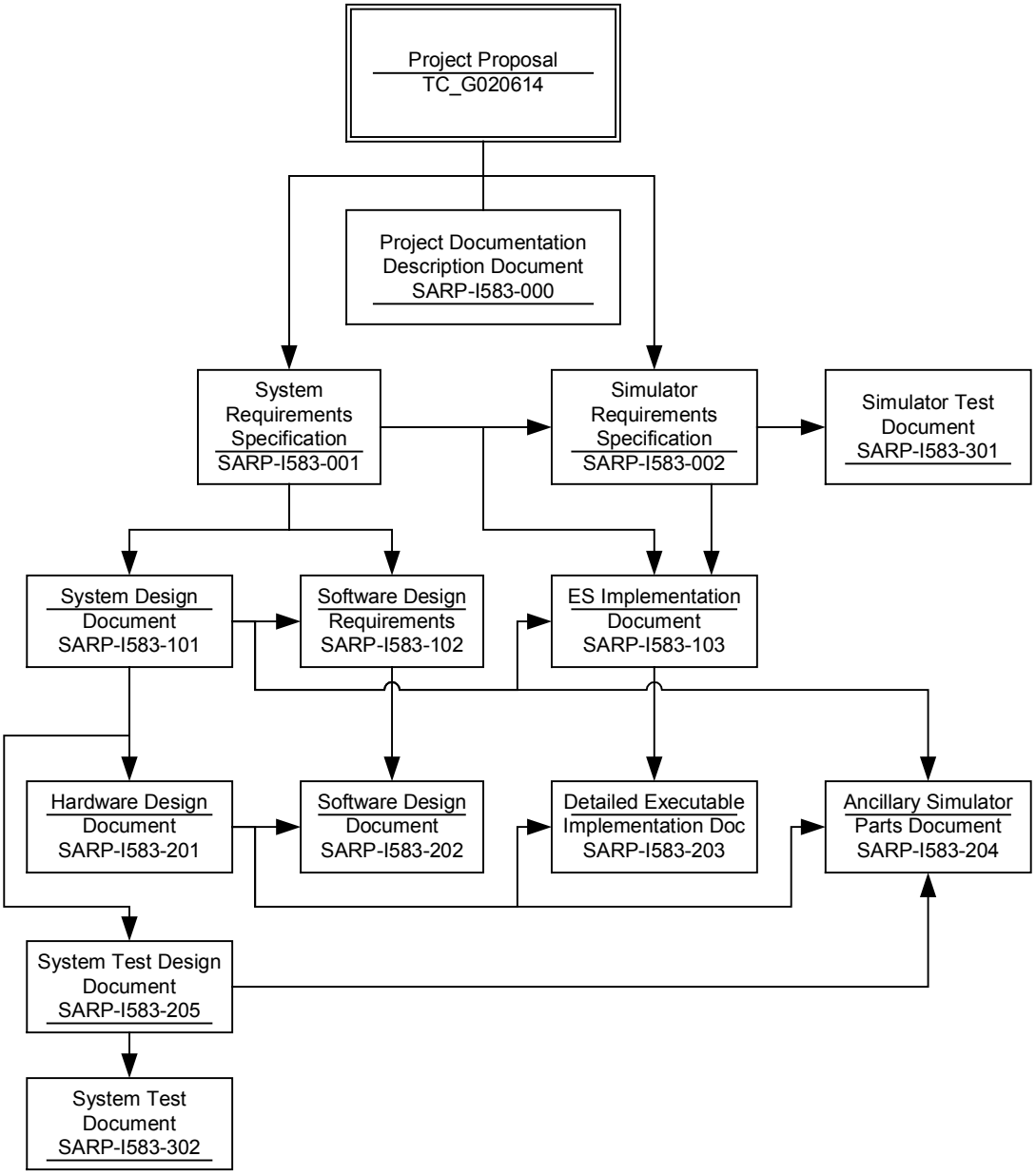

Figure 1: Document Relational Structure

3.2.2 SARP-I583-102 Software Design Requirements Document

The SDRD is used to document the software design developed to implement the functional requirements identified in the SyRS.

3.2.3 SARP-I583-103 ES Implementation Document

The ESID is developed to describe key implementation details of primary executable specifications. Separate documents are produced for each ES that will be developed into a DE. Descriptions of secondary ES' and other simulator parts are documented together in the Ancillary Simulator Parts Document.

3.3 Low-level Design Documents

3.3.1 SARP-I583-201 Hardware Design Document

The hardware design that will be developed to implement the system design described in the SyDD, is documented in the HDD. While no real hardware will be created for this project, the HW design will determine the environment for which the embedded SW will be developed. The HDD along with the ESID is a primary driver for the DE design.

3.3.2 SARP-I583-202 Software Design Document

The SDD is created to document the SW design developed to implement the requirements found in the SDRD. The SW design will execute on the HW design described in the HDD.

3.3.3 SARP-I583-203 Detailed Executable Design Document

The DE developed to run the executable software must function interchangeably in the virtual environment with its ES counterpart. The DE design documented in the DEDD, is based on the HW design described in the HDD and the ES implementation as described in the ESID.

3.3.4 SARP-I583-204 Ancillary Simulator Parts Document

This document lists all of the ancillary parts used in the virtual system and provides supporting descriptive detail where appropriate. These parts are developed from design details documented in the SyDD, the HDD, and the STDD.

3.3.5 SARP-I583-205 System Test Design Document

The STDD documents all of the tests developed to exercise the system design with the ES and also with the DE. Additional tests are required to exercise additional low-level functions that are not part of the core system functionality (e.g. built-in-test functions, etc.).

3.4 Test Documents

3.4.1 SARP-I583-301 Simulator Test Document

This document contains details on the tests that were used to verify the simulator itself, as well as the test results. When the simulator is used for V&V of commercial avionics SW, the FAA requires that all test tools used in support of avionics development comply with the verification requirements of DO-178B §12.2 as a SW-verification test tool. This document provides the tool qualification data for the simulator as required per DO 178B §12.2.3.

3.4.2 SARP-I583-302 System Test Document

The STD contains all of the test results produced from running the suite of system tests developed for the ES-based and DE-based systems, as documented in the STDD.